PROTECTING NETWORKS FROM ACCESS LINK FLOODING ATTACKS

ABSTRACT

Automated techniques are described that provide continuous, uninterrupted operation of the secure packet tunnels in spite of access link flooding attacks. A system is described that includes a source device and a destination device coupled to a network. The source and destination devices may comprise, for example, edge routers that couple local area networks to the network via access links. The source device and the destination device establish a packet tunnel that has a source network address and a destination network address. Upon detecting a network attack, the destination device selects a new network address for at least one of the source network address and the destination network address and establishes a new packet tunnel with the source device. The source network address and the destination network address may comprise port numbers, Internet Protocol (IP) addresses, or other information describing the source and destination devices.